IDENTIFICACION Y EXPLOTACION DE VULNERABILIDADES EN APLICACIONES WEB DE UN ENTORNO ACADEMICO

Presentado por:
Andres Fernando Castaneda Suarez

Tutores:
Ing. Angela Marcela Mejía fajardo, Ph.D.
Ing. Carlos Gilberto Delgado

Dirigido a:
Programa de Ingeniería en telecomunicaciones

Universidad Militar Nueva Granada
Bogotá, Colombia
2015

Tabla De Contenido

I. INTRODUCCIÓN

Hoy en día las pruebas de Hacking ético son esenciales para el control y verificación del estado de una infraestructura de red, desde sus grandes portales hasta las conexiones internas (Intranet o red privada), que muchas veces son blanco fácil para atacantes que aprovechándose de diversas amenazas y vulnerabilidades logran acceder y/o manipular información confidencial de una organización.

Con el desarrollo de la investigación se pretende describir una metodología simple que le permita a un evaluador o administrador de red, monitorear y analizar de un forma sencilla los sitios web que componen su red a través de procesos de recolección de información relacionada con el sitio, identificación de vulnerabilidades a través del uso de herramientas automatizadas, con el fin de explotar una vulnerabilidad en términos de acceso, escalabilidad de privilegios y daños.

En el documento [1], los autores definen diferentes procedimientos y configuraciones que hacen una aplicación y una red insegura, explorando diferentes vulnerabilidades. Además, exponen diferentes herramientas como Nessus Y OpenVas que permiten la exploración e identificación de vulnerabilidades. Proponen la implementación de ambientes virtualizados para la identificación de fallas de seguridad y aprendizaje controlado.

En la UAE University, proponen y apoyan la virtualización de entornos para el aprendizaje de técnicas y procedimientos relacionados con hacking ético, en el ambiente de pruebas denominado *DoS_VLab* que implementa tecnologías GNS3, virtual Box y VMware para simular diferentes servicio que son vulnerables a ataques de denegación de servicio y que son explicados en el documento [2].

II. PLANTEAMIENTO DEL PROBLEMA

Hoy en día todas las organizaciones cuentan con aplicaciones web y son cada vez más dependientes de ellas, si se llega a presentar un problema, por sencillo que sea puede llegar a detener y comprometer las operaciones de la organización. Por tanto, surge la inquietud y necesidad de conocer el nivel de exposición que presentan los servicios web de una institución u organización.

III. OBJETIVOS

General:
Realizar un análisis de seguridad en los servidores web de una organización, como resultado de la aplicación de la guía Web Applications Pentest (WAP) de OWASP.

Específicos

- Identificar las principales vulnerabilidades y estrategias de ataque en servidores web, implementando la distribución Kali Linux y la guía de Web Applications Pentest (WAP) de OWASP.

- Implementar un escenario de pruebas requerido que simule un servicio real, que permita explotar cada vulnerabilidad en términos de acceso, escalabilidad de privilegios y daños.

- Proponer y evaluar controles para mitigar las amenazas detectadas.

- Describir a través de una guía las técnicas y herramientas utilizadas, así como las vulnerabilidades, el alcance de las mismas y el nivel de gravedad.

IV. MARCO TEORICO

OWASP "(Open Web Applications Security Project): Comunidad de seguridad informática sin ánimo de lucro, dedicada a mejorar la seguridad de aplicaciones web y software en general. [3]", mediante el uso de:

• Herramientas y estándares de seguridad.

• Libros completos de revisiones de seguridad en aplicaciones.

• Controles de seguridad estándar y librerías.

• Extensas conferencias alrededor del mundo.

• Listas de correo.

GUIA DE EVALUACION DE OWASP:

El proyecto OWASP Testing ha sido desarrollado durante muchos años. El objetivo del proyecto es ayudar a las personas a entender: El qué, por qué, cuándo, dónde y cómo probar las aplicaciones web. La guía de OWASP, está diseñado para ayudar a las organizaciones a comprender qué compone un programa de pruebas y ayudarles a identificar los pasos que deben llevarse a cabo para construir y operar un programa de pruebas para aplicaciones web, esta guía puede utilizarse como una referencia y una metodología para ayudar a determinar la brecha entre las prácticas existentes y las mejores prácticas de la industria. Es por eso que la guía de evaluación de OWASP es considerada un documento que incluye "mejores prácticas" [4].

El modelo descrito en la guía de OWASP se divide en dos fases [5]:

- Fase 1 Modo Pasivo:

El evaluador intenta comprender la lógica de la aplicación y juega con la aplicación.

- Fase 2 Modo Activo:

En esta fase el evaluador implementa un conjunto de pruebas activas descritas en la guía de OWASP que se ha dividido en 11 categorías para un total de 91 controles:

- Recopilación de información
- Pruebas de gestión de configuración e implementación.
- Pruebas de gestión de identidad.
- Pruebas de autenticación.
- Pruebas de autorización.
- Pruebas de gestión de sesión.
- Pruebas de validación de ingreso.
- Manejo de errores.
- Criptografía.
- Pruebas de lógica del negocio.
- Pruebas del punto de vista del cliente.

HERRAMINETAS SPIDER

Spider es una funcionalidad que traen diferentes herramientas para explorar sitios web de una forma automática, a partir de una dirección inicial, el script descarga direcciones, analiza las pagina y busca enlaces a páginas nuevas o a directorios de configuración y diseño que permiten el funcionamiento del aplicativo. Dentro de esta clasificación se encuentran diferentes herramientas como Burp suite, ZAP ATTACK, Paros, entre otras más.

BUPR SUITE:

Es una herramienta para realizar procesos de seguridad de aplicaciones Web, cuenta con la integración de componentes que permiten realizar una auditoría a sitios web mal configurados y con errores en la programación. El software incluye las siguientes funcionalidades [6]:

- escáner para identificación de vulnerabilidades (versión pago).
- Spider con reconocimiento de aplicaciones, para el rastreo de dominios relacionados a la URL principal, subdominios, directorios de diseño y configuración de la aplicación
- Proxy que le permite inspeccionar y modificar el tráfico entre el navegador y la aplicación de destino.

- Una herramienta de intrusión, para realizar poderosos ataques personalizados para encontrar y explotar vulnerabilidades inusuales.

HERRAMIENTAS AUTOMATIZADAS:
Existe un número indeterminado de empresas y personas que ofrecen análisis de seguridad automatizado, estas herramientas son limitadas, son consideradas herramientas genéricas, que parten de una vulnerabilidad conocida, descubierta en la tecnología que implementa el aplicativo. Los problemas más graves de seguridad son catalogados como no genéricos, donde la vulnerabilidad se entrelaza con la lógica del negocio y el diseño de la aplicación personalizada. Estas herramientas automatizadas pueden apoyar procesos globales para producir una aplicación más segura, también pueden ser útiles en procesos de investigación de vulnerabilidades en una organización, como tarea rutinaria ayudando al personal de seguridad en sus tareas diarias [7].

ACUNETIX
Escáner automatizado, capaz de escanear cualquier sitio o aplicación Web, identifica vulnerabilidades de tipo[8]:

- inyección de SQL: Técnica donde un atacante crea o altera sentencias SQL para exponer datos ocultos, sobrescribir los mismos, o ejecutar comandos peligrosos a nivel de sistema en el equipo que hospeda la base de datos [9].

- Cross Site Scripting (XSS): Permite a un atacante inyectar código JavaScript o lenguaje similar, logrando saltar controles de seguridad para obtener datos, secuestrar sesión o comprometer el navegador de usuario [10].

- Otras vulnerabilidades a nivel de código y fallas de seguridad conocidas dependiendo de la tecnología implementada por el aplicativo web.

ZAPATTACK DE OWASP
Es una herramienta utilizada para el análisis de servicios web, cuenta con características que puede ser de gran ayuda al momento de realizar una evaluación a un aplicativo web. las principales ventajas con las que cuenta un auditor al utilizar esta herramienta son [11]:

- Herramienta gratuita.
- Herramienta multi-plataforma (Windows, Linux y MAC).
- Fácil de instalar.
- Gran variedad de manuales de ayuda y gran comunidad en la red.

La herramienta cuenta con diferentes funcionalidades, como son:

- Posibilidad de comprobar todas las peticiones y respuestas entre cliente y servidor.
- Posibilidad de localizar recursos en un servidor.
- Análisis automáticos.
- Análisis pasivos.
- Posibilidad de lanzar varios ataques a la vez.
- Análisis de sistemas de autenticación.

¿QUÉ ES UN WEB APPLICATIONS PENTEST?
WAP o evaluación de intrusión web, es un procedimiento de evaluación de la seguridad de un sistema de computadores (servicios) mediante la simulación de un ataque. Está enfocada solamente a evaluar la seguridad de una aplicación web. El proceso analiza de forma activa la aplicación en busca de cualquier debilidad, fallos técnicos o vulnerabilidades. Cualquier incidencia de seguridad será presentada al propietario del sistema, junto con una evaluación impacto, y una propuesta para mitigar la vulnerabilidad [12].

¿QUÉ ES UNA VULNERABILIDAD?
"Una vulnerabilidad es un defecto o debilidad en el diseño, implementación, operación o gestión de un sistema que podría ser explotado para comprometer los objetivos de seguridad del sistema" [13].

¿QUÉ ES UNA AMENAZA?
"Una amenaza es cualquier cosa (un ataque malintencionado externo, un usuario interno, una inestabilidad del sistema, etc.) que puede dañar los activos propios de una aplicación (recurso de valor como los datos en una base de datos o en el sistema de archivos) mediante la explotación de una vulnerabilidad" [14].

¿QUE ES UN EXPLOIT?
Es un programa artesanal que aprovecha una vulnerabilidad, en otros casos permite escalar privilegios en el sistema o eliminar información. Los Exploits dependen de los sistemas operativos y sus configuraciones, también de las configuraciones de los programas que se están ejecutando en un ordenador. Es importante recalcar que para la utilización y ejecución de un Exploit debe contar con la supervisión/aprobación del administrador del sistema porque puede ser considerado un delito y está penado con fuertes multas y/o cárcel [15].

FRAMEWORK METASPLOIT

Herramienta Open Source para el desarrollo y ejecución de Exploit contra una maquina remota. Metasploit, contiene multitud de herramientas y/o programas que permiten cumplir con tareas de escaneo, identificación de vulnerabilidades, módulos para ataques de fuerza bruta. El Framework tiene disponible diversos tipos de cargas útiles (o Payloads: que hace referencia al programa que realiza una acción adicional después de aprovechar la vulnerabilidad con el Exploit, por ejemplo: devolver una Shell) que son listan a continuación [16]:

- Shell de comandos: permite ejecutar comandos arbitrarios.
- Meterpreter: Permite ejecutar comandos y/o controlar la pantalla de un dispositivo mediante VNC, navegar, cargar y descargar archivos.
- Cargas dinámicas: permite a los usuarios evadir antivirus.

SEGURIDAD DE LA INFORMACION

La seguridad de la información corresponde a un conjunto de acciones preventivas y correctivas que toda organización debe realizar en sus sistemas tecnológicos y de información buscando mantener y salvaguardar la Disponibilidad, Confidencialidad e integridad [17]

DISPONIBILIDAD:
Capacidad que garantiza que el software es operativo y accesible por usuarios autorizados.

CONFIDENCIALIDAD:
Capacidad de preservar cualquier información y/o activos manejado, están ocultos a usuarios no autorizados.

INTEGRIDAD:
Capacidad que garantiza que el código del software y/o activos, configuraciones y comportamientos no puedan ser o no hayan sido modificados o alterados.

V. METODOLOGIA

En base a la guía de evaluación de OWASP, se plantea el siguiente procedimiento para llevar a cabo una evaluación o test de intrusión (Figura 1).

Figura 1. Metodología Para la evaluación de un sitio web.

En la imagen anterior (figura 1), se puede ver una metodología simple que puede implementar para evaluar la seguridad de un sitio web. La primer etapa corresponde al *Rastreo e Identificación De Información*, que consiste en la implementación de herramientas *Spider* (programas que inspecciona las páginas de un portal Web de forma metódica y automatizada*),* que permiten analizar el sitio, para identificar y descubrir la estructura completa de todos los directorios y archivos del aplicativo web.

En la segunda etapa denominada *Identificación de vulnerabilidades (figura 1), s*e ejecutan herramientas automatizadas capaces de lanzar una serie de ataques que permitan evaluar los controles de seguridad dispuestos en el sitio web, subdominio y directorios relacionado con la URL principal (ruta visible en la barra de texto del navegador, que ubica de manera precisa un servidor [18]).

Teniendo el informe de vulnerabilidades que entregan las herramientas automatizadas y otra información importante obtenida en la etapa de rastreo e identificación de información es necesario proceder con la etapa de *Explotación* (Figura 1*)* que le permite

conocer al evaluador el alcance y efectos que puede producir una vulnerabilidad en términos de acceso, escalabilidad de privilegios y daños.

VI. DISENO Y CONSTRUCCION PLATAFORMA DE PRUEBAS

Gracias a las tecnologías de hoy en día, es posible virtualizar una amplia variedad de sistemas operativos y aplicaciones para recrear entornos del objetivo, sin necesidad de recurrir a un hardware dedicado y lograr explotar parámetros de configuración y observar el comportamiento de la aplicación u objetivo sin conectarse directamente con el aplicativo real.

Para no afectar la Disponibilidad, Confidencialidad e integridad de los servicios de una organización, se acordó implementar un aplicativo que simule un servicio real. El servicio seleccionado corresponde a un sitio web con las siguientes características:

TECNOLOGIAS QUE SUSTENTAN EL SITIO WEB
JOOMLA 3.7.2
XAMPP 5.6.30
FRESSHD 1.2.6

Tabla 1. Tecnologías utilizadas para el diseño y configuración del sitio web.

En la Tabla 1, se listan las tecnologías que sustentan el aplicativo. A continuación, se realiza una breve descripción de cada uno de ellos:

JOOMLA: Es un sistema de gestión de contenidos (CMS) que permite desarrollar sitios web dinámicos e interactivos, con este tipo de aplicaciones es posible crear, modificar o eliminar todo tipo de contenido de un sitio web de manera sencilla a través de un panel de administración [19].

XAMPP: Es un servidor de plataforma libre, software que integra en una sola aplicación, un servidor web Apache, intérpretes de lenguaje de scripts PHP y un servidor de base de datos MySQL, que en conjunto permite desarrollar y compilar páginas web [20].

FREESHD: Software que permite instalar un servidor SSH en el sistema operativo y que permitirá controlarlo de forma remota sin dificultad.

La herramienta utilizada para la virtualización del servicio web es VMware Player, aplicación de licenciamiento libre que permite la instalación de máquinas virtuales. Se configuro una maquina con Sistemas Operativo Windows 8.1 (Figura 2), totalmente actualizado con soporte y parches para protegerse de las vulnerabilidades conocidas que afectan los sistemas Microsoft.

El esquema de red utilizado a lo largo de la investigación se presenta a continuación:

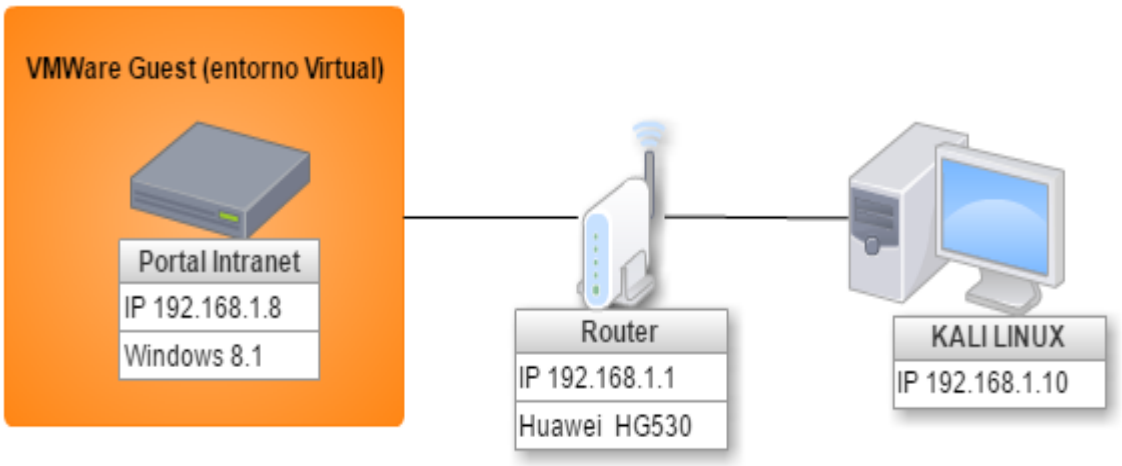

Figura 2. Esquema de red.

En la figura 2, se puede ver el esquema de red que fue diseñado para la investigación. aun lado está el sitio web que simula servicio real bajo la dirección 192.168.1.8 , todas las pruebas se realizaron bajo un red local utilizando como herramienta la distribución de Kali Linux (dirección IP 192.168.1.10), esta distribución de Linux se desarrolló con el fin de reunir las mejores herramientas para realiza pruebas de penetración y auditorias de seguridad, contiene diversas herramientas que están orientadas a diferentes tareas de Hacking, tales como pruebas de penetración, investigación de seguridad, computación forense e ingeniería inversa [21].

VII. RESULTADOS

RASTREO E IDENTIFICACIÓN DE INFORMACIÓN

Se encontraron diferentes subdominios, relacionados a la gestión del negocio como: Admisiones, paginas para realizar trámites y servicios, programas académicos, diferentes comunidades (estudiantes docentes y administrativos); dominios para pagos en línea; directorios y archivos relacionados con plugins que fueron configurados en el aplicativo para dar cierta personalización a la plantilla y dinamismo al sitio.

IDENTIFICACIÓN DE VULNERABILIDADES,

Las herramientas no identificaron ninguna vulnerabilidad sobre el sistema de gestión de contenido (CMS) de Joomla debido a que se configuro y se diseñó el sitio web con la última versión del CMS; tampoco se identificaron vulnerabilidades conocidas sobre la versión Windows. Pero si se identificó una vulnerabilidad en la versión del servicio SSH denominada *Remote Authentication Bypass*.

EXPLOTACIÓN DE VULNERABILIDADES:

Se explotó la vulnerabilidad, utilizando la herramienta METASPLOIT, que permitió obtener una Shell (que llamaremos sesión 1 y que utilizaremos más adelante), de comunicación con el servidor víctima como se muestra en la siguiente imagen (figura 3).

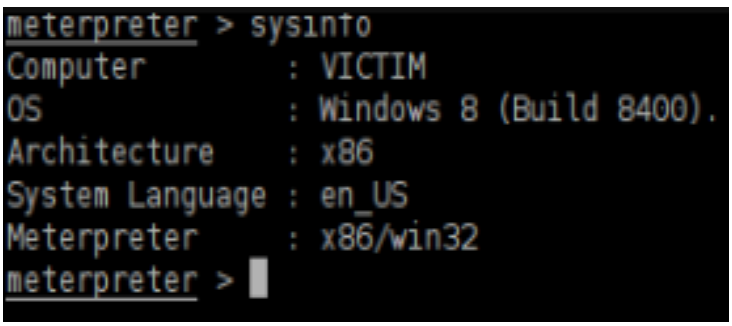

Figura 3. Shell de comunicación con el equipo víctima.

En la imagen anterior (figura 3), se puede ver la Shell obtenida después de aprovechar la vulnerabilidad *Remote Authentication Bypass*, y las características del sistema operativo del servidor que aloja el aplicativo web, a través del comando *sysinfo.*

VIII. ACCESO, ESCALABILIDAD DE PRIVILEGIOS Y DAÑOS

Teniendo acceso al sistema (sesión 1) es necesario revisar que privilegios de usuario se tienen sobre el servidor vulnerable, para esto *meterpreter* dispone del comando *getuid,* que permite hacer operaciones de consultas y manipulación de cuentas de usuario:

Figura 4. Instrucción para identificar el usuario con el que se compilo la Shell.

De la imagen anterior (figura 4), se puede ver el nombre del usuario (PRUEBAS-01760CC) y el grupo al que pertenece el mismo (Administrador) con el que se compilo la Shell dentro de la maquina víctima. Windows trabaja con diferentes perfiles de usuarios y grupos, en este caso el usuario pertenece al grupo Administrador, sin embargo, existe un perfil que tiene más privilegios, denominado SYSTEM que solo es utilizado por el sistema operativo y que tiene un nivel de jerarquía similar al usuario Root en distribuciones Linux. El comando disponible en meterpreter para escalar privilegios al usuario SYSTEM es *getsystem*:

Figura 5. Fallo para elevación de privilegios.

Sin embargo, de la figura 5, se puede ver que después de ingresar la instrucción en la consola de Metasploit, el Framework devuelve un mensaje indicando que la operación fallo y el acceso a la cuenta S*YSTEM* está protegido. Lo anterior se debe a que los sistemas Microsoft implementan la protección denominada *User Account Control* (UAC), que corresponde a una tecnología de seguridad que tiene por objetivo impedir que las aplicaciones maliciosas hagan cambios no autorizados en el ordenador; para deshabilitar este servicio, METSAPLOIT cuenta con el Exploit bajo la ruta *exploit/windows/local/bypassuac*. Para esto es necesario guardar la Shell anterior (sesión 1) a través del comando *background.* Y cargar el Exploit denominado "bypassuac" que para ejecutarse con éxito debe tener acceso al sistema (el cual se obtuvo en la sesión 1 y que se debe indicar al momento de configurar el módulo bypassuac a través de la instrucción *set sesión 1*). Para ejecutar el exploit que permite elevar privilegios es necesario escribir en la consola del Framework la instrucción Exploit o run.

En la siguiente imagen (figura 6), se puede ver la nueva Shell y después de ejecutar nuevamente el comando *getsystem,* permite aumentar privilegios a la cuenta del sistema.

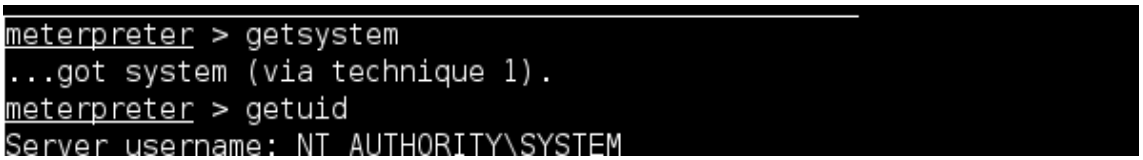

Figura 6. Elevación de privilegios usuario SYSTEM.

Con los privilegios que otorga la cuenta SYSTEM, un atacante tiene acceso a la carpeta SYSTEM VOLUME INFORMATION donde puede eliminar copias de seguridad o puntos de restauración del servidor, también tiene acceso total sobre ciertas claves de registro para el buen funcionamiento del servicio, un claro ejemplo son las Claves SAM, en donde se almacenan los datos de los usuarios existentes en el sistema y donde el atacante puede modificar las claves para secuestrar la cuentas disponibles en el servidor.

Utilizando diferentes instrucciones como*: cd y ls*, un atacante puede navegar por los directorios descargando diferentes archivos y directorios que le permitan obtener información valiosa de la organización, hasta llegar a la carpeta de configuración de Joomla ubicada en la ruta *C:\xampp\htdocs\joomla,* donde un atacante puede obtener, insertar, modificar y /o eliminar artículos, imágenes y documentos disponibles para los clientes del sitio. Por otro lado, puede eliminar los plugins o módulos con el fin de afectar la disponibilidad del Portal web.

IX. CONTROLES PARA MITIGAR LAS AMENAZAS:

Para contrarrestar la vulnerabilidad en el servicio freeSSHd es necesario actualizar a la última versión 1.3.1 del aplicativo disponible en [22]. Para su instalación realice el siguiente procedimiento:

- Descargar el programa de su página oficial.
- Clic derecho en instalar con permiso de administración.
- Se compila una serie de ventanas donde debe presionar el botón siguiente.
- Y por último el aplicativo le pregunta si quiere ejecutarlo como un servicio del sistema, en la que debe dar clic en el botón sí.

X. CONCLUSIONES

La metodología propuesta tiene un procedimiento altamente práctico, las herramientas son de fácil instalación y acceso, necesitan pocos requerimientos de hardware; la información identificada a través de las herramientas automatizadas es confiable.

La herramienta Acunetix, se instaló bajo su versión gratuita, sin embargo el informe de resultados es muy completo y certero, describiendo los puntos débiles que se presentan no solo en el sitio web sino en otras tecnologías que están instaladas bajo el mismo servidor, como fue el caso del servicio FREESSHD y la vulnerabilidad *Remote Authentication Bypass*, además no solo identifica donde se encuentra la falla de seguridad sino que también indica el diagnóstico del porque la debilidad y las recomendaciones de cómo solucionar la vulnerabilidad.

No existe una tecnología cien por ciento segura, pero es posible disminuir el riesgo de un ataque cibernético, si se cuenta con los sistemas actualizados, como fue el caso del sistema operativo del servidor y la versión de Joomla donde el aplicativo no encontró ninguna falla de seguridad.

Es importante ejecutar este tipo de herramientas con autorización previa del personal encargado de la infraestructura de comunicaciones de una organización ya que si no se cuenta con ella, puede ocasionarle problemas legales porque usted está intentando acceder a información que no es de su propiedad.

XI. BIBLIOGRAFIA

[1] Y. Wang and J. Yang, "Ethical Hacking and Network Defense: Choose Your Best Network Vulnerability Scanning Tool," 2017 31st International Conference on Advanced Information Networking and Applications Workshops (WAINA), Taipei, Taiwan, 2017, pp. 110-113. Disponible en: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7929663&isnumber=7929495

[2] S. A. Kaabi, N. A. Kindi, S. A. Fazari and Z. Trabelsi, "Virtualization based ethical educational platform for hands-on lab activities on DoS attacks," 2016 IEEE Global Engineering Education Conference (EDUCON), Abu Dhabi, 2016, pp. 273-280. Disponible en: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7474565&isnumber=7474513

[3] OWASP, "Guía De Prueba De Owasp", 2016, pp 5. Disponible en: https://www.owasp.org/images/1/19/OTGv4.pdf

[4] Owasp.org, (2015). OWASP Testing Project - OWASP. Retrieved November 2014, Disponible en: https://www.owasp.org/index.php?title=OWASP_Testing_Project&setlang=es#tab=Project_About

[5] OWASP, "Guía de Pruebas De Owasp V4", 2016, pp 28. Disponible en: https://www.owasp.org/images/1/19/OTGv4.pdf

[6] PortSwigger Ltd, "Getting Started With Burp Suite", 2017. Disponible en: https://portswigger.net/burp/help/suite_gettingstarted.html

[7] OWASP, "Guía de Pruebas De Owasp V4", 2016, pp 6. Disponible en: https://www.owasp.org/images/1/19/OTGv4.pdf

[8] Acunetix Ltd. "Product Manual". 2017. Disponible en: https://www.acunetix.com/resources/wvsmanual.pdf

[9] OWASP. "SQL Injection". 2017. Disponible en: https://www.owasp.org/index.php/SQL_Injection

[10] OWASP. "Top 10 2007-Secuencia de Comandos en Sitios Cruzados (XSS)". 2017. Disponible en: https://www.owasp.org/index.php/Top_10_2007-Secuencia_de_Comandos_en_Sitios_Cruzados_(XSS)

[11] Balderrama E. "OWASP Zed Attack ProxyGuide", 2016. Disponible en: https://www.gitbook.com/book/snifer/owasp-zed-attack-proxy-guide/details

[12] OWASP, "Guía de Pruebas De Owasp V4", 2016, pp 9-10. Disponible en: https://www.owasp.org/images/1/19/OTGv4.pdf

[13] Owasp.org,. OWASP Zed Attack Proxy Project - OWASP. Retrieved November 2014, Dsiponible en: https://www.owasp.org/index.php?title=OWASP_Zed_Attack_Proxy_Project&setlang=es

[14] OWASP, "Guía de Pruebas De Owasp V4", 2016, pp 28. Disponible en: https://www.owasp.org/images/1/19/OTGv4.pdf

[15] Nunez A. "que es un exploit?". 2016. Disponible en: http://www.seguridadjabali.com/2012/09/que-es-exploit.html

[16] Offensive-Securitty. "Tutorial de Metasploit Framework". 2014. Disponible en: https://radiosyculturalibre.com.ar/biblioteca/INFOSEC/Manual_de_Metasploit_Unleashed.pdf

[17] ISO 27001. "¿Qué significa la Seguridad de la Información?". 2015. Disponible en: http://www.pmg-ssi.com/2015/05/iso-27001-que-significa-la-seguridad-de-la-informacion/

[18] department of computer and information science. "What Is a URL?". 2010. Disponible en: https://www.cis.upenn.edu/~bcpierce/courses/629/papers/Java-tutorial/networking/urls/definition.html

[19] Joomla. "Joomla!® 3 Explained: Your Step-by-Step Guide (2nd Edition) (Joomla! Press)" . 2014. Disponible en: https://www.joomla.org/joomla-press-official-books.html

[20]Zapata C. "¿Qué es XAMPP y para qué sirve?". 2011. Disponible en: http://mantenimientosdeunapc.blogspot.com.co/2011/11/que-es-xampp-y-para-que-sirve.html

[21] Offensive Security. "what is Kali Linux?". 2017. Disponible en: http://docs.kali.org/introduction/what-is-kali-linux

[22] Freesshd. "Downloads". 2015. Disponible en: http://www.freesshd.com/?ctt=download